IDIS (2009) 2:363–368
DOI 10.1007/s12394-009-0034-2

Book Review: Ian Kerr, Valerie Steeves, Carole Lucock (Eds.), lessons from the identity trail (2009)

Andrea M. Matwyshyn

Received: 22 October 2009 / Accepted: 22 October 2009 / Published online: 8 December 2009

In what is undoubtedly to become a seminal interdisciplinary work in the field of information privacy policy and law, Lessons from the Identity Trail is a well-organized book, replete with detailed comparative analysis that spans five international jurisdictions. Editors Ian Kerr,[1] Valerie Steeves,[2] and Carole Lucock[3] have brought together a stellar group of Canadian and international academics and practitioners to engage in a thoughtful dialogue about the strengths and weaknesses of data protection law, various identity technologies, anonymity and related policy and legal issues. Although the compilation evidences a focus on Canada, its twenty-eight chapters include coverage of the information privacy regimes of the United States, Italy, the Netherlands and the United Kingdom for comparative purposes. Further this text is one of four texts arising from the broader work of over 50 co-investigators, collaborators, researchers and partners, funded by the Social Science Research Council Initiative on the New Economy. In short, this text is an essential acquisition for anyone engaged in serious study of the field of information privacy, identity or anonymity.

The book is divided into three major sections—privacy, identity and anonymity. In the first section on privacy, chapters one to eleven introduce the current state of Canadian privacy law and undertake discussions of legal fields pushing on the

[1]Ian Kerr holds the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa, Faculty of Law.

[2]Valerie Steeves is an Assistant Professor in the Department of Criminology and the Faculty of Law at the University of Ottawa.

[3]Carole Lucock is a doctoral candidate in the Law and Technology Program at the University of Ottawa, Faculty of Law.

A. M. Matwyshyn (✉)
Wharton School, University of Pennsylvania, Philadelphia, PA, USA
e-mail: amatwysh@wharton.upenn.edu

evolution of current doctrine in Canada. In Chapter 1, *Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent*, Kerr, Jennifer Barrigar,[4] Jacquelyn Burkell[5] and Katie Black[6] question the fulcrum of the Canadian privacy regime—the construction of meaningful consumer consent to data collection. Relying on insights from psychology and other interdisciplinary theory, they argue that PIPEDA's "withdrawal of consent" provisions will provide inadequate relief and call for a higher level of demonstrable consent in privacy law than that required in traditional contract law. Philippa Lawson[7] and Mary O'Donoghue[8] present another discussion of consent in Chapter 2, *Approaches to Consent in Canadian Data Protection Law.* They assert that a more nuanced understanding of the citizen-government relationship is required when analyzing data privacy and that overreliance on the idea of consent is undesirable. Chapter 3, *Learning from Data Protection law at the Nexus of Copyright and Privacy*, by Alex Cameron[9] engages in an analysis of the tensions between copyright law and intellectual privacy. He cautions that a disconnect can develop between data protection law analysis in certain cases and results that more broadly underscore the proper relationship between copyright and privacy under Canadian law. In Chapter 4, *A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments*, Robert Carey[10] and Jacquelyn Burkell place the privacy paradox—that users claim concern over privacy but yet reveal large amounts of information—in the context of digital social environments. They introduce several cognitive heuristics and argue that they may explain the privacy paradox in context of digital social environments.

Ann Utreck[11] raises issues related to privacy and ubiquitous computing in Chapter 5, *Ubiquitous Computing and Spatial Privacy.* She argues that the current Canadian constitutional approach to privacy protection is less efficacious in the context of a ubiquitous computing environment, where traditional spatial, personal and temporal boundaries are deconstructed, and a more successful approach must focus on something other than location in physical space. Chapter 6, *Core Privacy: A Problem for Predictive Data Mining* by Jason Miller discusses the unique threats to privacy he perceives to arise from predictive data mining. Distinguishing predictive data mining from descriptive data mining, he argues that predictive data mining brings with it potential violations of core privacy concerns. In Chapter 7, *Privacy Versus National Security: Clarifying the Trade-Off,* Jennifer Chandler[12]

[4] Jennifer Barrigar is a doctoral candidate in the Law and Technology Program at the University of Ottawa, Faculty of Law.
[5] Jacquelyn Burkell is an Associate Professor at the Faculty of Information and Media Studies, University of Western Ontario.
[6] Katie Black is an LLB candidate at the University of Ottawa, Faculty of Law.
[7] Philippa Lawson is the former Director of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa.
[8] Mary O'Donohue is the Senior Counsel and Manager of Legal Services at the Office of the Information and Privacy Commissioner of Ontario.
[9] Alex Cameron is a doctoral candidate in the Law and Technology Program at the University of Ottawa, Faculty of Law.
[10] Robert Carey is a Postdoctoral Fellow at the Faculty of Information and Media Studies, the University of Western Ontario.
[11] Anne Uteck is a doctoral candidate in the Law and Technology Program at the University of Ottawa, Faculty of Law.
[12] Jennifer Chandler is an Associate Professor at the University of Ottawa, Faculty of Law.

presents a cogent argument regarding why and how the value of security seems to trump the value of privacy. Chandler cautions against counterterrorism measures that merely create feelings of security while in reality creating new vulnerabilities. Daphne Gilbert[13] argues that privacy should best be understood as an aspect of equality in Chapter 8, *Privacy's Second Home: Building a New Home for Privacy* under Chapter 15 of the Charter. Through incorporating privacy under Section 15 of the Charter, a higher level of protection will pertain and demonstrate that privacy can be understood as fundamental to human dignity, says Gilbert.

Chapter 9, *What Have you Done for me Lately? Reflections on Redeeming Privacy for Battered Women* authored by Jenna McGill[14] calls attention to the overzealous rejection of privacy concerns in the context of battered women. Although privacy can be used incorrectly as an excuse for state nonintervention in a private home, privacy can also become a tool for battered women to use as part of their empowerment according to McGill. In Chapter 10, *Genetic Technologies and Medicine: Privacy, Identity, and Informed Consent,* Marsha Hanen[15] discusses the benefits and pitfalls of the use of genetic information in medical contexts. She warns about the potential abuse of information and the need to assess positive and negative implications of each use of genetic information, including crafting new methods of accountability where needed. Finally, Valerie Steeves in Chapter 11, *Reclaiming the Social Value of Privacy* leverages the insights of Westin's theory of privacy and those of multiple social theorists to propose a new model that defines privacy as a negotiation of interpersonal boundaries.

The second grouping of twelve chapters introduces a myriad of policy and legal debates surrounding construction of identity. Section II begins with Steven Davis[16] presenting a framework of identity that differentiates metaphyscial, epistemological and social/cutltural/political identities in Chapter 12, *A Conceptual Analysis of Identity.* Chapter 13, *Identity, Difference and Categorization* by Charles D. Raab[17] introduces two concepts of identity—commonality with others and group identification versus individuality and uniqueness. Similarly, it highlights the duality of identity as both defined by self and others in a form of negotiation. A. Michael Froomkin[18] takes the reader through a discussion of identity cards and the romantic imagery that has been used to create furor around them in Chapter 14, *Identity Cards and Identity Romanticism*. He then argues, however, that these romantic visions distract from the set of complex and critical data protection access and storage issues.

Chapter 15 shifts to questions of publication and identity in Jane Doe's[19] discussion entitled *What's in a Name? Who Benefits from the Publication Ban in Sexual Assault Trials.* The author questions whether a misplaced sense of shame

[13] Daphne Gilbert is an Associate Professor at the University of Ottawa, Faculty of Law.
[14] Jenna McGill is a clerk at the Supreme Court of Canada.
[15] Marsha Hanen is a former president of the University of Winnipeg and an Adjunct Professor of Philosophy at the University of Victoria.
[16] Steven Davis is Professor Emeritus of Philosophy at Simon Fraser University.
[17] Charles Raab is Professor Emeritus of Government at the School of Social and Political Studies at the University of Edinburgh.
[18] A Michael Froomkin is Professor of Law at the University of Miami, Faculty of Law.
[19] Jane Doe is an author, teacher and community organizer whose successful suit against the Toronto Police set legal precedent taught in law schools across Canada.

drives victim of rape to shield their identity when it is the perpetrator of the crime who should be shamed. She discusses the positives and negatives of anonymity from the perspective of victims of sexual assault using a series of interviews. In Chapter 16, *Life in the Fish Bowl: Feminist Interrogations of Webcamming,* Jane Bailey[20] tells the story of Jennicam, where one woman allowed an internet audience to watch her every move via webcam, and discusses differing feminist responses to it. Questions of identity and ubiquitous computing are analyzed in Chapter 17, *Ubiquitous Computing, Spatiality, and the Construction of Identity: Directions for Policy Response*, authored by David J. Phillips.[21] Phillips argues that identity is a negotiated performance of meaningful relationships and that ubiquitous computing can fundamentally alter this performance. He proposes "semiotic democracy" as an approach to policy responses. David Matheson[22] discusses automated identification and its pertinent privacy risks and dignity risks. Referencing Goffman's total institution, he warns of depersonalization through automation and identifies three types of dignity concerns in Chapter 18, *Dignity and Selective Self-Preservation.*

Chapter 19, *The Internet of the People? Reflections on the Future Regulation of Human-Implantable Radio Frequency identification*, Ian Kerr argues that current law in North America is not adequate to address the challenges presented by human-implantable RFID and human-machine merger. He suggests guidelines predicated on meaningful consent and consumer participation. Discussion next shifts to biometrics and immigration in Chapter 20, *Using Biometrics to Revisualize the Canada-US Border*, by Shoshana Magnet.[23] Magnet questions the implementation of biometric identification technologies on the US-Canada border and the accompanying narrative of security and efficiency. Gary Marx[24] discusses the connection between music and surveillance in Chapter 21, *Soul Train: The New Surveillance in Popular Music*. He identifies two competing forces: control agents and members of the surveillance industry, on the one hand, who view surveillance as an answer, and artists, on the other hand, who view surveillance as a problem. Chapter 22, *Exit Node Repudiation for Anonymity Networks* by Jeremy Clark,[25] Philippe Gauvin,[26] and Carlisle Adams[27] sets forth a method for node owners who have innocently passed on information connected with an offence to be able to assert they did not originate the communication and do not harbor information related to an offence. Finally, Section II on identity concludes with a discussion of surveillance and search engines, in Chapter 23, *TrackMeNot: Resisting Surveillance in Web Search* by Daniel C. Howe[28] and Helen Nissenbaum.[29] The authors discuss a Firefox browser extension called "TrackMeNot" which obfuscates user queries by using a stream of

[20] Jane Bailey is an Associate Professor at the Faculty of Law, University of Ottawa.
[21] David J. Philips is Associate Professor at the Faculty of Information, University of Toronto.
[22] David Matheson is an Assistant Professor in the Department of Philosophy at Carleton University in Ottawa.
[23] Jeremy Clark is a doctoral candidate with the Centre for Applied Cryptographic Research and the Cryptography, Security, and Privacy Group at the University of Waterloo.
[24] Shoshana Magnet is an Assistant Professor at the Institute of Women's Studies at the University of Ottawa.
[25] Gary Marx is Professor Emeritus of Sociology at MIT.
[26] Philippe Gauvin is counsel, regulatory affairs, for Bell Canada.
[27] Carlisle Adams is a Full Professor in the School of Information Technology and Engineering at the University of Ottawa.
[28] Daniel C. Howe is a digital artist, researcher and PhD student at NYU's Media Research Lab.
[29] Helen Nissenbaum is Professor of Media, Culture, and Communication at New York University.

programmatically generated decoys. They assert that the extension provides an option that enables both user expression and privacy without reliance on third parties in a technologically and socially complex environment.

The third and final section of LESSONS FROM THE IDENTITY TRAIL groups together five chapters on the state of the law and anonymity in various jurisdictions. A. Michael Froomkin conducts a review of the current state of law with regard to anonymity in the United States in Chapter 24, *Anonymity and the Law in the United States*. He assesses the United States Supreme Court's approach to anonymity as a patchwork evidencing a clash between conflicting policies woven into the federal structure—the need for protection from government and the need for government to identify potential wrongdoers—as well as a hesitation by courts to intervene in matters perceived to be governed by private contract. The discussion of the United States is immediately juxtaposed with a discussion of the state of the law regarding anonymity in Canada, authored by Carole Lucock and Katie Black in Chapter 25, *Anonymity and the Law in Canada*. The authors distinguish anonymity from privacy and present Canadian law as a piecemeal approach where recent security concerns are lessening opportunities for anonymity. Chapter 26, *Anonymity and the Law in the United Kingdom* by Ian Lloyd[30] presents an analysis of the similar issues in context of UK law. Referencing debates over issues such as identity cards and CCTV, the author concludes by pointing to the difficulty of crafting legal protections for privacy and anonymity if millions of people share their information at will: though consumers allege to value privacy, they fail to consider the privacy implications of sharing through loyalty card programs and social network sites.

Chapter 27, *Anonymity and Law in the Netherlands*, by Simone Van Der Hof,[31] Bert-Jaap Koops,[32] and Ronald Leens,[33] and Chapter 28, *Anonymity and the Law in Italy* by Giusella Finocchiaro[34] conclude the book with analysis of two continental approaches to anonymity, those of the Netherlands and Italy respectively. Chapter 27's authors conclude that the Dutch approach to privacy and anonymity is also a piecemeal one, and that creating a right to anonymous communications under Dutch law would be a logical extension. Finocchiaro points out that Italian law similarly does not have a unified approach in addressing anonymity. She argues that anonymity should be considered a type of privacy and data protection right that should be balanced with other fundamental rights. For Finocchiaro, technology can implement the rules of law once they are established.

This book presents an important contribution to the scholarship of information privacy law, and the next three volumes will undoubtedly likewise do so. In those subsequent volumes, an even greater focus on the role of corporate actors and corporate law would buttress the totality of the analysis. Although the perceptions of the individual with respect to privacy, identity and anonymity are of integral importance, the actualization of these perceptions into functional legal regimes is

[30] Ian Lloyd is Professor of Information Technology Law at the University of Strathclyde Law School.
[31] Simone Van Der Hof is a Senior Research Fellow and Assistant Professor at the Tilburg Institute for Law, Technology, and Society of Tilburg University.
[32] Bert-Jaap Koops is Professor of Regulation and Technology at Tilburg University.
[33] Ronald Leenes is an Associate Professor at the Tilburg Institute for Law, Technology, and Society at Tilburg University.
[34] Giusella Finocchiaro is Professor of Internet Law and Private Law at the University of Bologna.

greatly limited by the role of corporations; these private corporate actors seeking to generate revenue through data leveraging are a driving force in information policy today. The literature of information privacy needs to be expanded with extensive discussions of the role of corporate fiduciary duties, securities law, agency law and the obligations of companies, as well as individual officers and directors, to society and their shareholders with respect to consumer information. Similarly, the important discussions of contractual consent presented in this text will become even more useful when placed alongside future discussions of liability limitation, corporate information vulnerability and recourse for information harms arising out of corporate conduct. Further, particularly as the EU member states ponder how and whether to borrow the data breach notification regimes prevalent in the United States in their implementations of upcoming EU directives on information privacy, these regimes' efficacy requires scrutiny as well as greater analysis of what constitutes an optimal set of private and public sector data security duties. Finally, although this text was already international in focus and covered five countries' regimes, it focused on North American and EU perspectives exclusively. Inclusion of perspectives from Asia, South America, Australia, Africa and the Middle East in future volumes would further a truly global dialogue on issues of information privacy.